



Cisco Umbrella DNS Cisco Secure Access - DNS Defense

Cisco Secure Access
Updated August 28, 2026

第 1

章

:

- [Cisco Secure Access - DNS Defense](#)
- [Cisco Security Cloud Control](#)
- [Cisco Umbrella](#)

Cisco Umbrella を Secure Access - DNS Defense にアップグレードする前に、アップグレードガイド全体をお読みください。

アップグレードにかかる時間は、移行に必要なデータとポリシーの数によって異なります。このプロセス中も Cisco Umbrella は動作し続け、組織は常に保護されます。

Cisco Umbrella から Secure Access DNS へのアップグレードのビデオもご覧いただけます。アップグレードプロセス全体をステップごとに解説しています。

重要

Secure Access へのアップグレードを開始するには、完全な管理アクセスが必要です。

- [Cisco Secure Access - DNS Defense](#) へようこそ
- [QuickStart](#)
- [Cisco Security Cloud Control](#) アカウントの作成
- [Cisco Umbrella](#) でのアップグレードマネージャの作成
- [ガイドラインと制約事項](#)

このオファーは、Cisco Umbrella DNS Advantage、Cisco Umbrella DNS Essentials、MSP、Multi-org のお客様が利用できます。

このオファーは、Cisco Umbrella DNS Advantage、Cisco Umbrella DNS Essentials、MSP、Multi-org のお客様が利用できます。

注

Secure Access のトライアルライセンスは、このアップグレードではサポートされていません。アップグレードには、有効な有料の **Secure Access** サブスクリプションが必要です。トライアルライセンスを使用すると、期限切れになり、既存の **Cisco Umbrella** ダッシュボードへのアクセスが中断される可能性があります。

現在の **Cisco Umbrella** 製品を特定するには、管理対象組織の **Cisco Umbrella** ダッシュボードに移動し、[管理 (Admin)] > [ライセンス (Licensing)] を選択します。

Cisco Secure Access - DNS Defense

Cisco Secure Access - DNS Defense で強化されたセキュリティを体験してください。

DNS レイヤ保護だけにとどまらない機能を提供するように設計された **Secure Access** で、新しいセキュリティ時代に踏み出しましょう。この高度なソリューションは、最新の **DNS Advantage** または **Essentials** の機能を統合して包括的な保護を提供し、サイバー脅威の一步先を行くことを可能にします。オフィス、自宅、外出先のいずれから接続する場合でも、比類のない可視性と制御が得られるため、安心して接続できます。

注

Cisco Umbrella から **Secure Access - DNS Defense** にアップグレードする前に、アップグレードガイド全体を必ずお読みください。

Secure Access - DNS Defense を選ぶ理由

- シームレスな移行：運用を中断することなく、強化されたセキュリティ対策へスムーズにアップグレードできます。
- いつでもどこからでも接続：場所やデバイスを問わずアプリケーションやデータにセキュアにアクセスでき、リモートワークが容易になります。
- ゼロトラストアーキテクチャ：VPNを使用せずに社外ネットワークのリソースに接続して、プライベートアプリケーションを確実に保護します。
- きめ細かなアクセス制御：ユーザーロール、デバイスコンプライアンス、その他の重要な要因に基づいてアクセス権限を調整します。
- 多要素認証 (MFA)：複数の検証ステップによりセキュリティを強化して、許可されたアクセスのみを確立します。
- 堅牢なポリシーの適用：詳細なセキュリティポリシーを導入し、ユーザーアクセスとアクティビティを効果的に管理します。

Secure Access は、企業アプリケーションへのセキュアで信頼性の高いアクセスが不可欠なリモートワークのシナリオにおける理想的なパートナーです。ユーザーアクセスとアクティビティの制御を強化することで、内部リソースを安心して保護できます。

このトピックでは、**Cisco Umbrella** から **Secure Access** へ移行する際に役立つベストプラクティスについて説明します。

Cisco Umbrella から **Secure Access** への移行に役立つベストプラクティスは次のとおりです。

- 業務時間外にアップグレードします。
- 移行ツールを使用して、一度に一部のデバイスを移行します。この段階的なアプローチにより、全面的な運用開始に拡大する前に、少数のデバイスグループで移行を検証できます。
段階的に移行することで、残りのデバイスを移行する前に、ポリシーをテストし、正常に統合できることを確認し、問題があれば解決できます。
- **トラフィックのリダイレクト**機能を使用すると、一度に一部のアイデンティティをリダイレクトできます。段階的なアップグレードアプローチをお勧めします。これにより、次のことが可能になります。
 - 少数のアイデンティティグループでインターネット アクセス ルールをテストする。
 - インターネット アクセス ルールが正常に統合できることを確認する。
 - 問題があれば早期に特定して対処する。

アップグレードを完了するために必要な手順の簡単な概要を示します。

1. **Cisco Security Cloud Control (SCC)** アカウントを作成します。**Secure Access** アカウントを **Cisco Umbrella** インスタンスにリンクするには、サブスクリプション要求コードが記載されたウェルカムメールを受信している必要があります。「[Cisco Security Cloud Control アカウントの作成](#)」の手順に従ってください。
詳細については、『[Security Cloud Control Getting Started Guide for Existing Customers](#)』の「[Claim a Subscription](#)」を参照してください。
2. **アップグレードマネージャのアクティブ化**。
3. **Cisco Umbrella** ダッシュボードですべての前提条件を満たします。
 - すべてのユーザーに対して **Cisco Security Cloud Sign On** を有効にします。
 - 仮想アプライアンスを更新し、**Active Directory** コネクタを更新します。
 - **Chromebook** を更新し、モバイルデバイスを更新します。
4. **アップグレードを開始**
Cisco Umbrella DNS ポリシーとコンポーネントが **Secure Access** のインターネット アクセス ポリシーおよび設定にコピーされます。
5. **トラフィックのリダイレクト**

組織のアイデンティティトラフィックをリダイレクトして、Cisco Secure Access を介して送信元としてステアリングされるようにします。

6. アップグレードを完了して Umbrella を閉じる

最後のステップでは、Cisco Umbrella アカウントを閉鎖し、Secure Access - DNS Defense のみを使用します。

Cisco Security Cloud Control

Cisco Security Cloud Control は、単一の統合インターフェイスからセキュリティ製品を管理し、セキュリティの成果を達成できるようにする新しいセキュリティプラットフォームです。

Cisco Security Cloud Control (SCC) は、シスコのセキュリティ製品の可視性と管理を一元的に提供します。Cisco Umbrella DNS から Secure Access - DNS Defense にアップグレードするには、要求コードが記載されたウェルカムメールを受信した後に、Security Cloud Control アカウントを作成する必要があります。詳細については、「[Signing in to Security Cloud Control](#)」を参照してください。

このプロセスの一環として、Security Cloud Sign On アカウントを作成します。Security Cloud Sign On は、1 組のログイン情報で複数の Cisco セキュリティサービスおよびクラウドサービスにアクセスするためのソリューションです。

最後に、セキュリティ強化のために多要素認証を設定する必要があります。Duo の使用を推奨します。

-
1. Security Cloud Sign On アカウントを作成して、[Security Cloud Control](#) (SCC) アカウントを作成します。
 2. [今すぐ登録 (Sign up now)] をクリックして、Security Cloud Sign On アカウントを作成します。

Security Cloud Sign On

Email

Continue

Don't have an account? [Sign up now](#)

3. [アカウントのサインアップ (Account Sign Up)] ページに情報を入力します。

Account Sign Up

Provide following information to create organization account.

[Back to login page](#)

Email *

First name *

Last name *

Country *

Password *

Show

Confirm Password *

Show

☒ By accept, you agree that your use of this Cisco Offer, and any Cisco Offers managed through this Cisco Offer, is governed by [Cisco's General Terms](#), and any applicable Offer Description(s) and Supplemental Terms. You also acknowledge that you have read the [Cisco Privacy statement](#).

Sign up

Password Requirements

- ✓ At least 8 character(s)
- ✓ At least 1 number(s)
- ✓ At least 1 symbol(s)
- ✓ At least 1 lowercase letter(s)
- ✓ At least 1 uppercase letter(s)
- ✓ Does not contain part of username
- ✓ Does not contain 'First name'
- ✓ Does not contain 'Last name'

4. アカウントをアクティブ化するための確認メールを確認してください。リンクは7日後に期限切れになります。



Welcome to Cisco Security Cloud Sign On (Preview)

Hi Username1,

Welcome to Security Cloud Sign On (Preview). Security Cloud Sign On is the single sign-on solution for Security Cloud products. To activate your account and get started, click **Activate account**.

Activate account

Link expires in 7 days.

For help activating your account, see the [documentation](#).

For additional help, contact our support team at tac@cisco.com or 1-800-553-2447 (US & Canada). You can find regional support numbers on the Cisco [support](#) site.

5. 多要素認証に登録します。Duo の使用を推奨します
6. SCC にユーザーを追加します。「[Role-Based Access Control in an Organization](#)」を参照してください。
すべての Cisco Umbrella 管理者を追加して、Cisco Umbrella からロックアウトされないようにします。アイデンティティ サービス プロバイダーを設定しない限り、すべてのユーザーを Duo に登録する必要があります。
7. [アイデンティティ サービス プロバイダー](#)を統合するには、次の手順を実行します。
8. 新しい組織名を作成します。

Create new organization

New organization name *

50 character limit

Region deployment *

This selection determines the deployment for all products and services added to this organization. [Read documentation](#).

Create

新しい **Secure Access** 組織の名前は、**Cisco Umbrella** 組織と同じにする必要があります。組織とリージョンの詳細については、「[Create an Organization](#)」を参照してください。

ドロップダウンメニューから任意のリージョンを選択します。この製品はグローバルに利用可能であるため、選択内容が製品の機能に影響することはありません。

Cisco Umbrella ダッシュボードにアップグレードマネージャを追加するには、次の手順を実行します。

Cisco Umbrella

アップグレードマネージャをアクティブ化する方法について説明します。

- **Cisco Umbrella** でアップグレードマネージャをアクティブ化する管理者は、**Security Cloud Control (SCC)** アカウントを作成する際に同じメールアドレスを使用する必要があります。別のメールアドレスを使用すると、**Cisco Umbrella** 組織を正しい **SCC** アカウントにリンクできなくなり、アップグレードが失敗して、**Cisco Umbrella** 組織がリンクされていない新しい **Secure Access** 組織が作成されます。
- 管理者は、**Secure Access - DNS Defense** にアップグレードするための固有のサブスクリプション要求コードが記載されたウェルカムメールを **Cisco Security Cloud** から受信する必要があります。
- サブスクリプション要求コードを受信した管理者は、**Cisco Umbrella** でアップグレードマネージャをアクティブ化するための後続の手順を完了する責任があります。

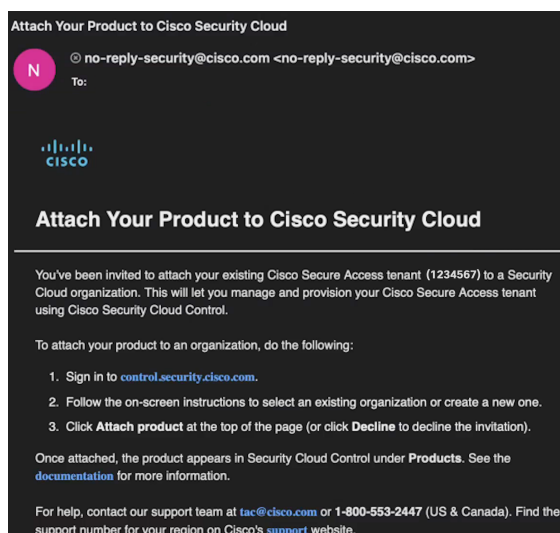
1. **Cisco Umbrella** アカウントにログインします。
2. [管理 (Admin)] > [ライセンス (Licensing)] > [Secure Accessへのアップグレード (Upgrade to Secure Access)] に移動し、[招待の要求 (Request Invitation)] をクリックします。

Upgrade to Secure Access

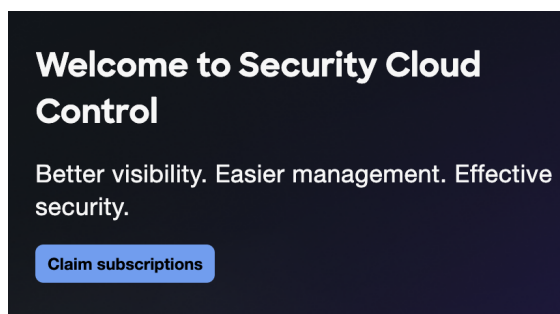
Once purchased, to begin the upgrade to Secure Access process, click Request Upgrade. You'll receive an email invitation that includes a code for you to attach in Security Cloud Control. For more information, see Umbrella's [Help](#).

REQUEST INVITATION

3. メールで [製品を Cisco Security Cloud にアタッチ (Attach Your Product to Cisco Security Cloud)] への招待を確認します。



4. このメール内のリンクをクリックして、**Security Cloud Control** アカウントにログインします。アップグレードマネージャをアクティブ化する **Cisco Umbrella** 管理者は、**Security Cloud Control** アカウントを作成する際に同じメールアドレスを使用する必要があります。
5. [サブスクリプションの要求 (Claim subscriptions)] をクリックします。



6. [Cisco Secure AccessインスタンスID (Cisco Secure Access Instance ID)] が **Cisco Umbrella** 組織 ID と同じであることを確認します。

Cisco Secure Access
Instance ID 8323335

7. [製品をアタッチ (Attach product)] をクリックし、次に [アタッチ (Attach)] をクリックして、**Cisco Umbrella** 組織を **Secure Access** インスタンスにアタッチします。

この操作を取り消すことはできません。

Invitations to attach existing product ⓘ 1

Cisco Secure Access
Instance ID 8262388

Decline Attach product

8. [サブスクリプションの要求 (Claim subscription)] をクリックし、サブスクリプション要求コードを入力します。

9. [次へ (Next)] をクリックして、サブスクリプション要求のワークフローを開始します。
10. ドロップダウンリストで [既存のインスタンスのアタッチ (Attach existing instance)] を選択します。

新しいインスタンスを作成しないでください。新しい組織は **Secure Access - DNS Defense** にアップグレードされません。

11. [要求 (Claim)] をクリックして、サブスクリプションIDや製品ライセンスなどのサブスクリプションの詳細を新しい **Secure Access** 組織に関連付けます。

サブスクリプションが正常に要求されました。製品のアクティベーションが完了するまでに数分かかる場合があります。製品が完全にアクティブ化されたら、左側のナビゲーションまたは **SCC** ページ上部にあるプラットフォームナビゲータから製品にアクセスできます。



Subscription successfully claimed.

It may take a few minutes for your products to complete activation. Once your products are fully activated, you can access them from the left-hand navigation or the platform navigator at the top of the page.

12. [製品およびサービスのアクティベーションステータス (Product and service activation status)] で、[アクションが必要 (Action required)] をクリックします。

13. [ライセンスの適用 (Apply license)] をクリックして、**Cisco Secure Access** を既存の **Cisco Umbrella** アカウントにリンクします。

Cisco Secure Access DNS Advantage

Subscription ID Sample-SecureAccess-Sub-001

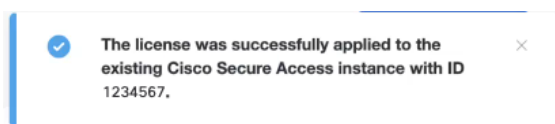
Apply license to an existing instance

The following Cisco Secure Access DNS Advantage instances are associated with your Cisco Security Cloud organization. Select an instance and click **Apply license**.

☒ **Cisco Secure Access** Externally managed
Instance ID 8262388

Cancel Apply license

ライセンスが **Cisco Secure Access** インスタンスに正常に適用されたことが通知されます。



14. Cisco Umbrella ダッシュボードにログインして、左側のナビゲーションに [アップグレードマネージャ (Upgrade Manager)] が表示されることを確認します。



15. 新しい **Secure Access** 組織を作成する前に、[アップグレードマネージャ (Upgrade Manager)] をクリックして、必要な前提条件を満たすプロセスを開始します。

次のステップとして、[前提条件 (Prerequisites)] を確認してから、[アップグレードの開始 (Start Upgrade)] に進み、新しい **Secure Access** 組織を作成します。

Cisco Secure Access - DNS Defense のガイドラインと制限事項について詳細を確認してください。

Cisco Umbrella Secure Access

アップグレードの開始の手順を完了すると、Cisco Umbrella アプリケーション設定は **Secure Access** アプリケーションリストになります。アプリケーション設定とアプリケーションリストは個別に管理され、この 2つのダッシュボード間ではアプリケーションカテゴリに加えた変更が反映されません。アップグレードマネージャの最後の手順を完了し、Cisco Umbrella アカウントを完全に閉鎖するまでは、変更を加えないことをお勧めします。

Cisco Umbrella でのアクセスのブロックと許可に関するアプリケーション設定が、Secure Access では 2つのアプリケーションリストに分割されます。Secure Access のインターネットアクセスルールをサポートするために、アプリケーションリストにはブロックまたは許可のみが含まれます。

Cisco Umbrella

- アイデンティティを含まない Cisco Umbrella DNS ポリシーは、Secure Access にコピーされません。

- 無効になっている **Cisco Umbrella DNS** ポリシーは **Secure Access** にコピーされ、無効のままになります。
- **Secure Access** はインテリジェントプロキシをサポートしていません。このレベルの **DNS** セキュリティを再現するには、**Secure Access** サブスクリプションを、同等レベルの **DNS** レイヤ保護である **Secure Access - DNS Defense** にダウングレードするか、**Secure Access** にアップグレードして、**Secure Access Secure Web Gateway** (SWG) を導入することをお勧めします。SWG では、より包括的なセキュリティ態勢を提供する完全な **Web** プロキシ機能を設定できます。

[Security Profiles] [SaaS Internet and SaaS Resources] Cisco Umbrella

アップグレードが開始されると、アップグレードマネージャの手順 4 を完了して **Cisco Umbrella** アカウントを閉鎖するまで、**Secure Access** では **Cisco Umbrella** ポリシーの [削除 (Delete)] 機能が無効になります。さらに、[セキュリティプロファイル (Security Profiles)] と [インターネットと SaaS のリソース (Internet and SaaS Resources)] にリストされている **Cisco Umbrella** ポリシーコンポーネントは、アップグレードマネージャがアクティブになっている間は **Secure Access** で削除できません。

Deletion of this List is disabled in Secure Access. Please navigate to the Umbrella Dashboard to manage deletions.

Delete

ブロックページバイパスはコピーされません。Secure Access 機能の詳細については、「[Manage Notification Pages](#)」を参照してください。

カスタムユーザーロールはコピーされません。Secure Access には、次の 2 つのロールのみがあります。

- 完全な管理者
- 読み取り専用

詳細については、「[Add a New Account](#)」を参照してください。

内部ドメイン許可リストは、[接続 (Connect)] > [エンドユーザー接続 (End User Connectivity)] > [インターネットセキュリティ (Internet Security)] > [トラフィックステアリング (Traffic Steering)] に移動して確認できます。

Secure Access

Secure Access ポリシーはルールベースであり、各ルールは最大 **250 個の一意の送信元アイデンティティ** をサポートします。**Cisco Umbrella** ポリシー [%POLICY NAME%] が **Secure Access** に変換されたときに、その結果生成されるルールがこの制限を超える可能性があります。移行を続行できます。ただし、**Cisco Umbrella** ポリシーに **250** を超える一意の送信元アイデンティティが含まれている場合、移行に失敗する可能性があります。

ポリシーが送信元アイデンティティとして [すべて (All)] を使用する場合は、この警告を無視しても問題ありません。たとえば、[すべてのローミングコンピューター (All Roaming Computers)] が選択されている

場合、**Cisco Umbrella** ポリシーには **250** を超えるカウントが表示されることがありますが、この選択は単一の送信元アイデンティティとして変換されます。

SaaS

[インターネットとSaaSのリソース (Internet and SaaS Resources)] ページには、インターネット アクセス ルールの設定時に宛先として使用できる再利用可能なコンポーネント (「オブジェクト」とも呼ばれる) が含まれています。インターネットおよびSaaSのリソースには、次のものが含まれます。

- [接続先リスト](#)
- [アプリケーションリスト](#)
- [コンテンツカテゴリリスト](#)

Cisco Umbrella

レガシー **Cisco Umbrella** コンテンツカテゴリは、**Secure Access** の同等のものにアップグレードされます。詳細については、「[Available Content Categories](#)」を参照してください。

Cisco Secure Access セキュリティプロファイルは、アクセスポリシーのルールで使用できる再利用可能なコンポーネントです。インターネットアクセスルール用のセキュリティプロファイルには、セットで設定するセキュリティ管理およびその他の設定 (アクセプタブルユースコントロールなど) が含まれています。詳細については、「[インターネットアクセス用のセキュリティプロファイルの追加](#)」を参照してください。セキュリティプロファイルには、次のものが含まれます。

- [脅威カテゴリ](#)
- [ファイル検査](#)
- [セーフサーチ](#)
- [復号除外リスト](#)
- [通知ページ](#)

Cisco Umbrella の選択的復号化は、**Secure Access** の [復号除外リスト (Do Not Decrypt List)] にアップグレードされます。アップグレードマネージャの実行中は、**Cisco Umbrella** で作成されたポリシーにリンクされている [復号除外リスト (Do Not Decrypt List)] に変更を加えることはできません。このオプションは、**Cisco Umbrella** アカウントを閉鎖すると有効になります。詳細については、「[Enable the Intelligent Proxy](#)」および「[Do Not Decrypt Lists](#)」を参照してください。

Intelligent Proxy Settings

Intercepts and proxies access requests to uncategorized or "grey" domains. [Help](#)

☒ Enabled

Gain visibility into threats, content, or apps by proxying web connections for risky domains.

☒ SSL Decryption

Enables Intelligent Proxy traffic inspection over HTTPS, HTTPS URL blocking, and blocks custom URLs in detention lists.

Do Not Decrypt Lists (optional)

0 - DAPI Validation Test

List of content categories, applications, and domains that are excluded from inspection. See [Do Not Decrypt Lists](#)

Secure Access では、[接続 (Connect)] > [ユーザー、グループ (Users, Groups)] > [設定管理 (Configuration Management)] > [ディレクトリの統合 (Integrate Directories)] > [IdP] の順に移動すると、[静的キー (Static Key)] が見つかります。詳細については、「[Provision Token for Identity Provider](#)」を参照してください。

Cisco Umbrella API

Cisco Umbrella API は 2022 年にリリースされたため、レガシー API キーは Secure Access に転送されません。Secure Access では、API キー、KeyAdmin キー、および静的キーを引き続き使用します。詳細については、「[Manage API Keys](#)」および「[Secure Access API Authentication](#)」を参照してください。

第2章

:

- Cisco Security Cloud Sign On □□□□
- □□□□□□□□□□□□□□□□
- Active Directory □□□□□□□□□□
- Chromebook □□□□
- □□□□□□□□□□□□

Secure Access - DNS Defense にアップグレードする前に、すべての前提条件を満たす必要があります。

Secure Access - DNS Defense にアップグレードする前に、すべての前提条件が満たされていることを確認してください。

1. Cisco Security Cloud Sign On の有効化
2. 仮想アプライアンスの更新および Active Directory コネクタの更新
3. Chromebook の更新およびモバイルデバイスの更新

1

Prerequisites

Not Started

Complete these steps before beginning the upgrade process. If you have previously completed a step, mark it as done.

✓

1. Enable Cisco Security Cloud Sign On

Enable Security Cloud Sign On as your authentication method.

Start

✗

2. Update VAs and AD connectors

Update your virtual appliances and Active Directory Connectors to their latest versions.

☐ Mark as done

Start

📱

3. Update Chromebooks and mobile devices

Update your Chromebooks and mobile devices to their latest versions.

☐ Mark as done

Start

Next

 注

アップグレード前に、レガシーAPIを使用して、他にも登録済みネットワークデバイスがあれば追加します。レガシーAPIを使用したネットワークデバイスの設定に関するガイダンスについては、<https://securitydocs.cisco.com/docs/umbrella-sig/olh/152032.dita> で「Hardware integration」セクションを参照してください。

 注

Cisco Umbrella DNS 専用パッケージから **Secure Access - Essentials** または **Secure Access - Advantage** にアップグレードし、**Secure Access - DNS Defense** にはアップグレードしない場合は、移行前に既存の Cisco Umbrella DNS ポリシーでインテリジェントプロキシを無効にします。

DNS 専用からフル Secure Access への移行中、Cisco Umbrella DNS インテリジェントプロキシは、DNS 専用の導入で使用される選択的プロキシではなく、フルプロキシにアップグレードされます。移行後の予期しないプロキシ動作を回避するため、事前にインテリジェントプロキシを無効にすることを推奨します。

Cisco Security Cloud Sign On

このトピックでは、Cisco Security Cloud Sign On を有効にし、Cisco Umbrella 管理者用の Security Cloud Control アカウントを作成する方法について説明します。

Cisco Security Cloud Sign On (SCSO) を使用すると、任意のデバイスから 1 組のログイン情報で各種 Cisco Security 製品にアクセスできます。Security Cloud Control は、単一の統合インターフェイスからこれらの製品を管理し、セキュリティ成果を達成するためのプラットフォームです。一方、Cisco Security Cloud Sign On は、これらの製品全体にわたってシームレスな認証を提供します。

- 完全な管理者ユーザーロールが必要です。
- **既存の SAML 設定**：組織が Cisco Umbrella ですでにアイデンティティプロバイダー (IdP) を使用している場合は、この機能を有効にする前に、Security Cloud Control で同じ IdP を設定する必要があります。これにより、既存の認証フローが維持され、管理者のロックアウトを防ぐことができます。明示的に要求されない限り、既存の Cisco Umbrella IdP 設定を削除しないでください。
- **ユーザーアカウントの確認**：Cisco Umbrella 管理者アカウントが、手動で作成されたユーザーまたは IdP を通じてプロビジョニングされたユーザーとして、Security Cloud Control にも存在することを確認します。アクセスで問題が発生しないように、Cisco Umbrella と Security Cloud Control の両方で同じ管理者メールアドレスを使用します。

詳細については、『Security Cloud Control Getting Started Guide for Existing Customers』の「[Overview of Security Cloud Sign On](#)」を参照してください。

1. アップグレードマネージャに移動します。Cisco Security Cloud Sign On の有効化前提条件ステップで、[開始 (Start)] をクリックします。

Upgrade To Cisco Secure Access

This upgrade process involves migrating data and configurations to you

0/4 steps complete

1

Prerequisites

Complete these steps before beginning the upgrade process

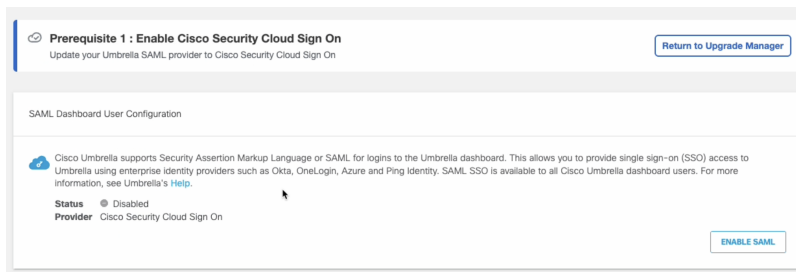
✓

1. Enable Cisco Security Cloud Sign On

Enable Security Cloud Sign On as your authentication method.

Start

2. [SAMLの有効化 (Enable SAML)] をクリックします。



3. 現在の設定に基づいて、次のいずれかの操作を実行します。

- **SAML が設定されていない場合** : [\[Cisco Security Cloud Sign On\]](#) をクリックして、すべての Cisco Umbrella ダッシュボードユーザー用に **Security Cloud Sign On** アカウントを作成します。次のウィンドウで、[\[今すぐ登録 \(Sign up now\)\]](#) をクリックします。アカウントの作成の詳細については、「[Invite a User](#)」を参照してください。

Step 1 of 3

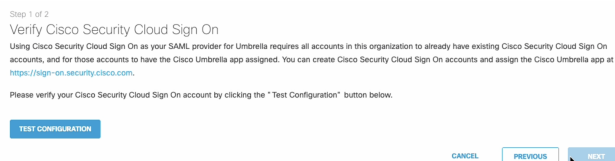
Select Umbrella SAML Provider

Select the SAML provider you'd like to authenticate users to Umbrella.

- ☒ Cisco Security Cloud Sign On
- ☐ PingID
- ☐ Okta
- ☐ OneLogin
- ☐ Azure
- ☐ Other

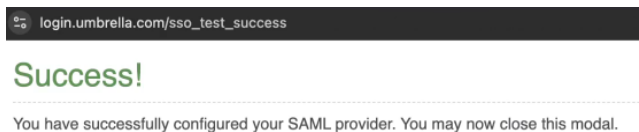
- **SAML がすでに設定されている場合** : 既存の IdP が **Security Cloud Control** で設定されていることを確認してから、アカウントのリンクに進みます。

4. アカウントが作成されたら、[\[アップグレードマネージャ \(Upgrade Manager\)\]](#) > [\[前提条件 \(Prerequisite\)\]](#) > [\[Cisco Security Cloud Sign Onの有効化 \(Enable Cisco Security Cloud Sign On\)\]](#) > [\[開始 \(Start\)\]](#) に戻ります。[\[Test Configuration\]](#) をクリックします。



セットアップを完了するには、[\[設定のテスト \(Test Configuration\)\]](#) を実行し、正常に完了する必要があります。

認証が完了すると、成功モーダルが表示されます。



5. [\[次へ \(Next\)\]](#) をクリックします。両方のチェックボックスをオンにして情報を確認し、[\[保存してユーザーに通知 \(Save and Notify Users\)\]](#) をクリックします。

Step 2 of 2

Save and Notify

After clicking 'Save', all users in your organization will be required to use the single sign-on service rather than a password. Umbrella will send an email to every administrative user in the dashboard, stating their password has been removed from their account.

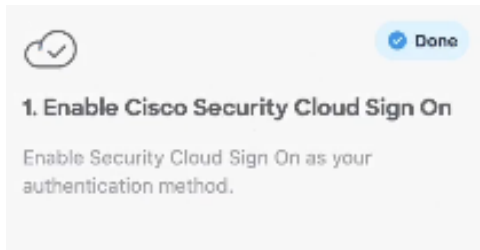
- ☒ If you disable the single sign-on service in the future, all users in your dashboard will be emailed a link to reset their passwords and their old passwords are not restored.
- ☒ Block page bypass users will no longer work once SAML is enabled. Instead, you must use codes for bypassing block pages. For more information, [read here](#).

Two step verification with Umbrella is not available when SAML is enabled. Instead, use the two factor options available with your SSO provider.

PREVIOUS

SAVE AND NOTIFY USERS

6. [アップグレードマネージャに戻る (Return to Upgrade Manager)] をクリックすると、[Cisco Security Cloud Sign On] の有効化 (Enable Cisco Security Cloud Sign On) ステップが [開始 (Start)] から [完了 (Done)] に変わります。



次の手順に従って、仮想アプライアンスと **Active Directory** コネクタが最新の状態であることを確認します。

Cisco Security Cloud Sign On を有効にした後：

- 今後、**Cisco Security Cloud Sign On** は **Cisco Umbrella** ダッシュボードユーザーにとって必須のサインイン方法になります。
- **Cisco Umbrella** は、すべてのダッシュボードユーザー（エンドユーザーを除く）に電子メールを送信して、シングルサインオン（SSO）が必須になり、パスワードが受け付けられなくなったことを通知します。
- 後で **SSO** が無効になった場合、以前のパスワードは無効になっているため、すべてのユーザーにパスワードをリセットするためのリンクが記載された電子メールが送信されます。
- **SAML** が有効になると、ブロック ページ バイパス ユーザーは機能しなくなります。

仮想アプライアンスが更新されていることを確認してください。

新しい仮想アプライアンス（VA）ソフトウェアバージョンは自動的に利用可能になり、通常は介入を必要とせずに適用されます。**DNS** サービスの高可用性を確保するには、自動更新を行うために **2** 台の **VA** が稼働している必要があります。

コネクタと **VA** はどちらも自動更新に対応しています。更新をダウンロードするには、これらのコンポーネントが次の **URL** にアクセスできる必要があります。

- **disthost.opendns.com** への **443**（TCP）
- **disthost.umbrella.com** への **443**（TCP）

リリースノートなど今後のバージョンの詳細については、「[Service Updates](#)」を参照してください。更新通知を受け取るには、[フォロー (Follow)] をクリックします。

仮想アプライアンスの更新は通常自動的に行われますが、手動で行うこともできます。

VA を v3.7.1 以降に更新し、[認証の強化 (Enhance Authentication)] を設定することを推奨します。

新しいバージョンを VA に自動的にインストールするには、**少なくとも 2 台の VA がインストールされている必要があります**。更新プロセス中にダウンタイムやサービスの中断が発生しないように、2 台の VA を配置しておく必要があります。

VA の「インプレース」手動更新を実行すると、最大 **15 分のダウンタイム**が発生します。その間、ネットワーク上で DNS クエリを実行できず、事実上、インターネットサービスを利用できません。

仮想アプライアンスを更新するには、次の手順を実行します。

- [仮想アプライアンスの更新](#)
- [仮想アプライアンスの認証の設定](#)

Active Directory

Active Directory コネクタが更新されていることを確認します。

Cisco Active Directory (AD) コネクタは、Cisco Umbrella と統合して、組織からユーザーとグループをプロビジョニングします。LDAP Interchange Format (LDIF) ソースファイルを使用してユーザーとグループをプロビジョニングするように AD コネクタをインストールおよび設定できます。サーバーに LDIF ファイルを展開すると、AD コネクタによって組織内のユーザーとグループが Cisco Umbrella と同期されます。

Active Directory

AD コネクタの自動更新を設定する手順を示します。

展開済みの AD コネクタ上の Cisco AD Connector ソフトウェアを Cisco Umbrella が更新する日時をスケジュールします。スケジュールすると、AD コネクタのソフトウェアが最新バージョンであるか Cisco Umbrella によってチェックされます。新しいバージョンが使用可能な場合、インストールされている AD コネクタソフトウェアが Cisco Umbrella によってシステムから削除され、AD コネクタの最新バージョンが展開されます。

Cisco Umbrella での完全な管理アクセスが必要です。

1. [展開 (Deployments)] > [設定 (Configuration)] > [サイトと Active Directory (Sites and Active Directory)] に移動し、[設定 (Settings)] をクリックします。
2. [Active Directory コネクタの自動アップグレード (Active Directory Connector Auto-Upgrades)] に移動し、[編集 (Edit)] をクリックします。
3. [曜日 (Day)] で、AD コネクタソフトウェアを更新する曜日を選択します。

 注

デフォルトの [曜日 (Day)] は [任意の日 (Any day)] です。ソフトウェアの更新が利用可能な場合は毎日、Cisco Umbrella によって、ソフトウェアの最新バージョンを使用して AD コネクタの再展開が試行されます。

4. [時間範囲 (Time Range)] で、スケジュールされた日に AD コネクタを更新する 4 時間単位の期間を選択します。

 注

デフォルトの [時間範囲 (Time Range)] は、午前 2 時～午前 6 時 PST です。

Chromebook

すべての Chromebook および Cisco Chromebook クライアントが更新されていることを確認します。

すべての Chromebook オペレーティングシステムと Chromebook クライアントが更新されていることを確認します。Chromebook のソフトウェアの更新は、Google が担当します。シスコが Chrome ウェブストアで Cisco Security for Chromebook クライアントを更新すると、Google 社によってすべての Chromebook にアップグレードが自動的にプッシュされます。このプロセスには数時間かかることがあります。詳細については、「[Chromebook Client FAQs](#)」を参照してください。

- Chromebook オペレーティングシステムをバージョン 122 以降に更新します。
- Cisco Security for Chromebook クライアントを 2.1.1 以降に更新します。

アップグレードを試行する前に、すべてのモバイルデバイスおよびクライアントが最新のものであることを確認します。

アップグレードを試行する前に、すべてのモバイルデバイスおよびクライアントを最新のものにします。モバイルデバイスまたはクライアントが設定されていない場合は、次の手順に進んでもかまいません。

詳細については、「[Managed Android Device](#)」を参照してください

詳細については、「[Managed iOS Device](#)」を参照してください

詳細については、「[Unmanaged Mobile Device Protection](#)」を参照してください

第3章

章

:

- **Secure Access - DNS Defense** □□□□ □□□□
- □□□□□□ □□□□ □□□ □□□□ □□□□□□
- **Secure Web Gateway** □□□□□□□□ □□□□□□□□□□

この手順では、新しい **Secure Access** 組織を作成し、**Cisco Umbrella** 設定をコピーします。

アップグレードプロセスを開始すると、新しい **Secure Access - DNS Defense** 組織が生成されます。このプロセス中も **Cisco Umbrella** は動作し続け、組織は常に保護されます。

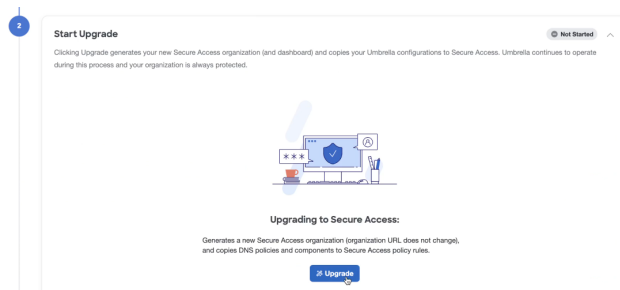
Cisco Umbrella DNS ポリシーおよびコンポーネントは、インターネットアクセスルール、設定、インターネットと **SaaS** のリソースとして **Secure Access** にコピーされます。アップグレード後、**Cisco Umbrella DNS** ポリシーは **Secure Access** で複数のルールに分割される場合があります。意図したとおりにトラフィックが処理されることを確認するために、ルールの順序を確認してテストする必要があります。

Secure Access - DNS Defense

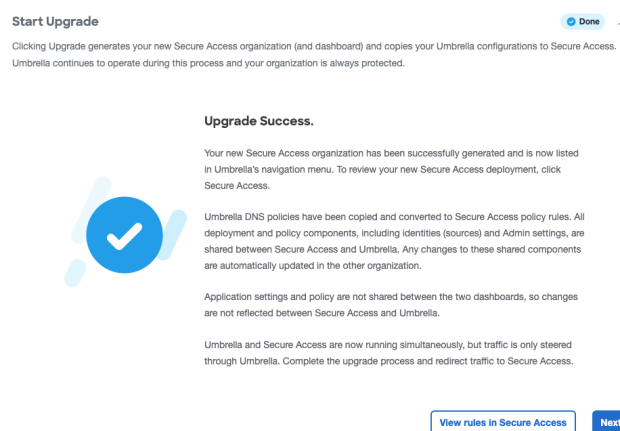
[アップグレード (Upgrade)] をクリックすると、新しい **Secure Access** 組織が生成され、**Cisco Umbrella** の設定がコピーされます。

Cisco Umbrella から **Secure Access** へのアップグレードの進行中は、ポリシーを変更しないことをお勧めします。ポリシーへの意図しない変更を避けるため、アップグレードが完了するまで既存のセキュリティプロファイルを編集または削除しないでください。移行後に **Cisco Umbrella** で作成されたポリシーは、**Secure Access** と同期されません。新しいポリシーコンポーネントのマッピングについては、「[Get Started with Internet Access Policy](#)」を参照してください。

1. [アップグレード (Upgrade)] をクリックして開始します。アップグレード中はページを終了しないでください。すべての変更が失われ、最初からやり直す必要があります。アップグレードにかかる時間は、**Cisco Umbrella** から **Secure Access** にコピーされるポリシーの数によって異なります。

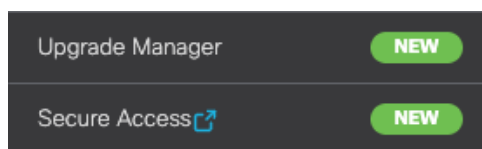


2. アップグレードが完了すると、[アップグレード成功 (Upgrade Success)] が表示されます。新しい **Secure Access** 組織が正常に生成されました。



3. [Secure Accessでルールを表示 (View rules in Secure Access)] をクリックして新しい **Secure Access** ダッシュボードに移動するか、[次へ (Next)] をクリックして[トラフィックのリダイレクト (Redirect Traffic)] に移動します。

次回 **Cisco Umbrella** にログインすると、左側のナビゲーションに **Secure Access** のショートカットが表示されます。



Cisco Umbrella ポリシーが **Secure Access** のルールとしてコピーされていることを確認します。新しいマッピングの詳細については、「[インターネット アクセス ルール](#)」を参照してください。

ルールの作成方法の詳細については、「[インターネット アクセス ルール スタートアップガイド](#)」を参照してください。

4. [アップグレードに失敗しました (Upgrade Failed)] と表示された場合は、[アップグレード (Upgrade)] をもう一度クリックするか、[サポート](#)にお問い合わせください

次の手順で、Cisco Umbrella アイデンティティの **Secure Access** へのリダイレクトを開始します。

アップグレード中の **Secure Access** に関する重要なログイン手順

アップグレードマネージャがアクティブな間は、Cisco Umbrella ダッシュボードからのみ **Secure Access** にアクセスしてください。

Cisco Secure Access で直接ログインすると、リダイレクトループが発生する可能性があり、サポート対象外です。ステップ 4 の「[アップグレードを完了して Cisco Umbrella を閉じる](#)」が完了するまでは、Cisco Umbrella ダッシュボードがサポートされる唯一のログイン方法です。

Cisco Umbrella DNS ポリシーは、アクセスポリシー内の **Secure Access** インターネット アクセス ルールになりました。

Cisco Umbrella から **Secure Access** にアップグレードすると、ポリシーの構造が変更されていることがわかります。Cisco Umbrella ではポリシーに複数のブロックコンポーネントと許可コンポーネントを含めることができますが、**Secure Access** では統合ポリシーモデルが採用されています。このモデル内の各ルールは、トラフィックをブロックまたは許可するように設定できます。移行中、Cisco Umbrella ポリシーは、次の特定の順序に従って、**Secure Access** で最大 3 つの個別のルールに変換されます。

1. 許可ルール（プライマリ）：最初のルールは、元の Cisco Umbrella ポリシーで指定されているトラフィックを許可する許可ルールです。
2. ブロックルール（セカンダリ）：2 番目のルールは、元の Cisco Umbrella ポリシーで定義されているトラフィックに制限を適用するブロックルールです。
3. 許可ルール（デフォルト）：ポリシー評価が Cisco Umbrella のポリシーモデルと一貫するように、3 番目のルールが暗黙的な許可ルールとして導入される場合があります。このルールは、宛先に対する明示的な一致が見つからないシナリオに対応し、意図しないトラフィックの中断を防ぎます。

非終端許可：暗黙的な許可ルールをサポートするため、**Secure Access** では非終端許可機能が導入されました。この機能により、デフォルトルールは次のようになります。

- ルール評価が適用側で終了せず、トラフィックをさらに分析できます。
- デフォルトで、安全で悪意のない Web サイトへの一般的なアクセスを許可します。シスコの脅威インテリジェンスによって悪意があると明示的にフラグ付けされない限り、Web サイトは許可されます。
- デフォルトルールは、カスタムルールが設定されるまで、元の Cisco Umbrella ポリシーのすべての送信元に適用されます。

- 宛先は [任意 (Any)] に設定されています。

デフォルトルール of 動作 :

- 非終端許可ルールが一致した場合、同じクエリサイクル中に、そのルールより後のルールは評価されません。
- ただし、**CNAME** レコードを分析しているときや、**DNS** 解決から解決済み IP アドレスを取得した後など、特定の状況下では同じクエリの評価を続けることができます。

注

送信元は、これらの新しく分割されたルールでも同じままです。

Cisco Umbrella ポリシーが Secure Access ルールにアップグレードされました

例 : [新規ポリシー (New Policy)] という名前の **Cisco Umbrella** ポリシーには、アイデンティティとして **AD** グループ、**AD** ユーザー、**AD** コンピューターがあります。コンテンツカテゴリにより、成人向け関連のすべての **Web** サイトと違法行為がブロックされ、アプリケーション設定により、**Box** クラウドストレージが許可されます。

Cisco Umbrella ポリシーが **Secure Access** のアクセスポリシーに表示されます。

- 1 つ目のルールの名前は、[3/3新規ポリシー (Umbrella) (3/3 New Policy (Umbrella))] です。送信元 : **AD** グループ、**AD** ユーザー、**AD** コンピューター。許可アプリケーションリスト : **Box** クラウドストレージ。
- 2 つ目のルールの名前は、[2/3新規ポリシー (Umbrella) (2/3 New Policy (Umbrella))] です。送信元 : **AD** グループ、**AD** ユーザー、**AD** コンピューター。ブロック コンテンツ カテゴリ リスト : 成人向け関連のすべての **Web** サイトと違法行為。
- 3 つ目のルールの名前は、[1/3新規ポリシー (Umbrella) (1/3 New Policy (Umbrella))] です。送信元 : **AD** グループ、**AD** ユーザー、**AD** コンピューター。[任意 (Any)] を許可します。[非終端許可 (Non-terminal Allow)] を表示するには、[セキュア (Secure)] > [アクセスポリシー (Access Policy)] > [デフォルト (Umbrella) (Default (Umbrella))] ルールの横にある [編集 (Edit)] をクリック > [セキュリティの設定 (Configure Security)] > [次へ (Next)] > [詳細設定 (Advanced)] > [非終端許可 (Non-terminal Allow)] に移動します。

☐	#	Rule name	Access	Action	Sources	Destinations	Security	Hits	Status
☐	1	3/3 New Policy (Umbrella)	Internet	Allow	Any AD Group... +2	Default Sett... +2	🌐	-	✓
☐	2	2/3 New Policy (Umbrella)	Internet	Block	Any AD Group... +2	Alcohol +16	🌐	-	✓
☐	3	1/3 New Policy Default (Umbrella)	Internet	Allow	Any AD Group... +2	Any	🌐	-	✓

Advanced

Do not change settings in this section unless you have a specific reason to do so. If you expect changes to be temporary, have a plan in place to ensure that you revert the changes.

☐ Allow access to encrypted files

Because encrypted files cannot be inspected for threats, downloading encrypted files is blocked by default. You should only allow access to encrypted files from trusted destinations. [Help](#)

☐ Override Security

Do not enforce the following configured security features for this rule: Handling of web traffic based on threat category; file inspection; and file type blocking. (Intrusion prevention (IPS) is NOT affected.) [Help](#)

☒ Non-terminal Allow

Allow rule will not terminate processing on the enforcement side allowing for additional analysis. [Help](#)

詳細については、「[Get Started With Internet Access Rules](#)」および「[Manage the Access Policy](#)」を参照してください。

1:

Cisco Umbrella ポリシーコンポーネント	Secure Access インターネット アクセス ルール
ポリシー	インターネット アクセス ポリシー
アプリケーションの設定	アプリケーションリスト
ブロックページの表示	通知ページ
コンテンツカテゴリ	コンテンツカテゴリ
接続先リスト	接続先リスト
アイデンティティ	送信元
モバイルデバイスおよびローミングコンピューター	ローミングデバイス
セキュリティ設定	脅威カテゴリ
選択的復号化	復号除外リスト

Secure Web Gateway

SWG が有効になっている場合のルール適用について説明します。

注

ここで説明するすべての機能がすべての Secure Access パッケージで使用できるわけではありません。現在のパッケージを確認するには、[管理 (Admin)] > [サブスクリプション (Subscription)] に移動します。詳細については、「[Determine Your Current Package](#)」を参照してください。

ここに記載されている機能にアクセスできない場合は、営業担当者に詳細をお問い合わせください。「[Cisco Umbrella and Cisco Secure Access packages](#)」を参照してください。

Cisco Umbrella から Cisco Secure Access にアップグレードするときに、組織で Secure Web Gateway (SWG) が有効になっている場合、ルール適用が変更されます。Secure Access では、SWG プロキシが、宛先に URL (example.com/login) が含まれているルールを最終的に適用します。

ブロックルールが URL に一致する場合、DNS リゾルバは完全な URL パスを評価できず、ドメイン (example.com) のみを識別できます。この場合、Secure Access は適用を SWG に委ねます。

- 1. DNS 評価：**宛先 (example.com/login) を評価するための要求。DNS リゾルバは、ドメイン (example.com) のみを認識し、適用を SWG に委ねます。
- 2. SWG に適用を委ねる：**ブロックページ (通知ページ) を返す代わりに、Secure Access は宛先 IP アドレスを返し、SWG が Web トラフィックを傍受して HTTP レイヤまたは HTTPS レイヤでブロックを適用するものと想定します。
- 3. SWG はトラフィックパス内に存在する必要がある：**ブロックを適用するには、ネットワーク トンネルグループ、PAC ファイル、または Cisco Secure Client を使用して、ユーザートラフィックを SWG 経由でステアリングする必要があります。
- 4. SWG を使用しない場合の結果：**トラフィックが DNS 専用パスに従い、SWG を通過しない場合、ブロックは適用されず、トラフィックは許可されます。

ルールを組織全体で一貫して適用するには、次の手順に従います。

1. **明示的なドメイン名を使用する**：ドメイン全体に適用する場合は、ドメイン（`example.com`）を宛先リストに追加します。特定の URL（`example.com/login`）を使用する場合、URL ベースで適用するには Web レイヤの検査が必要になるため、そのトラフィックは SWG 経由で評価されます。
2. **SWG の対象範囲を確保する**：URL ベースのブロックが必要な場合は、対象の送信元またはネットワークのデータパスで SWG プロキシがアクティブになっていることを確認します。Secure Access でこれを行うには、インターネットセキュリティを設定し、Cisco Secure Client、PAC ファイル、またはネットワーク トンネル グループを使用して Secure Access プロキシ経由でトラフィックをルーティングします。
3. **ルールを監査する**：特定の URL パスに依存するブロックルールを特定します。ルール設定をネットワークアーキテクチャに合わせることで、予期しない許可動作を防止し、セキュリティルールが意図したとおりに適用されるようにできます。

SWG 適用を設定するさまざまな方法については、『Cisco Secure Access Help guidebook』の次のトピックを参照してください。

- [Configure Cisco Secure Client Settings](#)（ローミングデバイスの場合）。
- [Manage PAC Files](#)。
- [Configure DNS and Web Security](#)（Web セキュリティポート 80/443 のトラフィックのみを有効化）。
- [Manage Network Tunnel Groups](#)（サイト、ブランチ、またはネットワークベースのトラフィックの場合）。

その他のリソースについては、次を参照してください。

- [インターネット アクセス ルールのトラブルシューティング](#)。
- [カスタム URL へのアクセスの制御](#)。
- [例](#)。
- [接続先リストの管理](#)。

第

4

章

:

- □□□□□□□□□□□□□□□□

組織のトラフィックを **Secure Access** 経由でリダイレクトする方法について説明します。

この手順では、トラフィックを **Secure Access** にリダイレクトする **Cisco Umbrella** アイデンティティを選択します。リダイレクト後、これらのアイデンティティからのトラフィックは、**Secure Access** のみを経由してルーティングされます。**Secure Access** では、アイデンティティはソースと呼ばれます。

アップグレードマネージャがアクティブな間は、**Secure Access** で登録済みネットワークやローミングデバイスなどの新しいソースを直接作成した場合でも、**Cisco Umbrella** のアップグレードマネージャに戻って、「ステップ 3：トラフィックのリダイレクト」を完了する必要があります。

これが必要になるのは、**アップグレードマネージャ**機能により、新規および既存のソースが、リダイレクトされるまで **Cisco Umbrella** アカウントに接続されたままになるためです。

Secure Access ダッシュボードに完全に移行するには、次の手順を実行します。

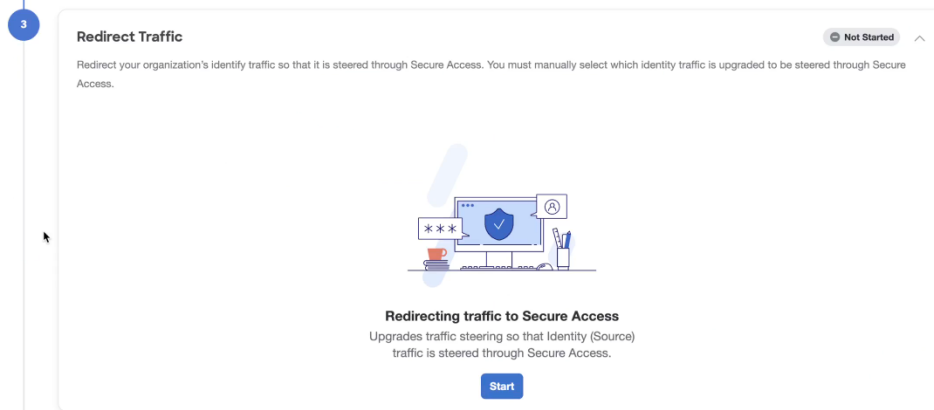
- ステップ 3：トラフィックのリダイレクト - **Cisco Umbrella** アイデンティティを **Secure Access** ソースにリダイレクトします。
- ステップ 4：アップグレードを完了して **Cisco Umbrella** を閉じる - **Cisco Umbrella** アカウントを無効化し、完全に閉鎖します。

Umbrella Secure Access

Cisco Umbrella のアイデンティティトラフィックをリダイレクトして、**Secure Access** 経由でのステアリングを開始します。

この手順では、**Cisco Umbrella** から **Secure Access** にトラフィックを切り替えます。この手順では、アップグレードを完了して **Cisco Umbrella** アカウントを閉じるまで、いつでもトラフィックを元に戻すことができます。必要に応じて、**Cisco Umbrella** で新しいアイデンティティを作成して、**Secure Access** の機能をテストすることもできます。

1. [トラフィックのリダイレクト (Redirect Traffic)] で、[開始 (Start)] をクリックします。



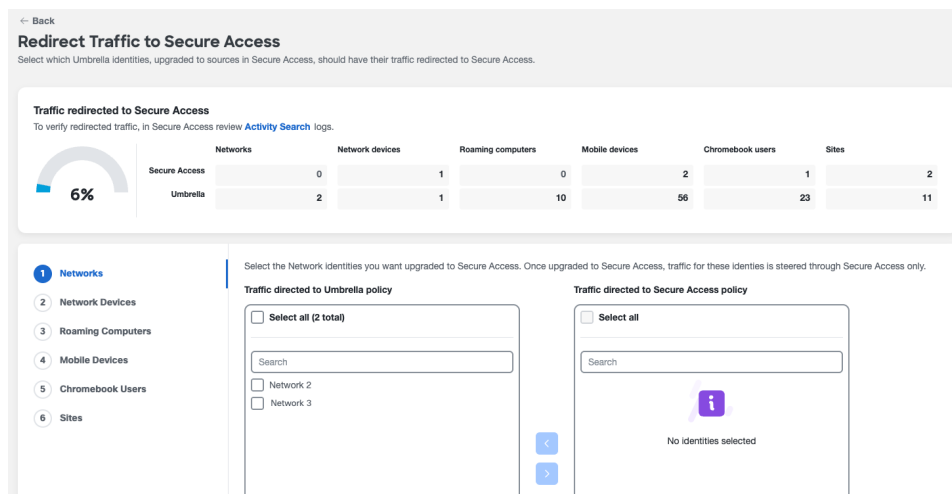
[Secure Accessへのトラフィックのリダイレクト (Redirect Traffic to Secure Access)] ページには、**Secure Access** にリダイレクトできるトラフィックを含む次のアイデンティティタイプが表示されます。

- ネットワーク
- ネットワークデバイス
- ローミングコンピュータ
- モバイルデバイス

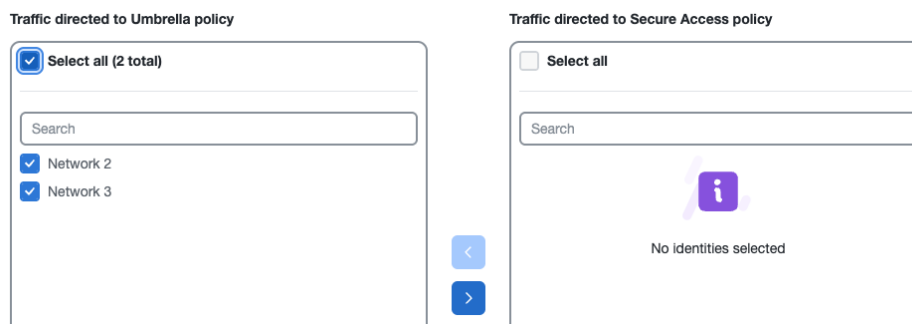
- Chromebook ユーザー
- サイト

2. アイデンティティタイプをクリックします。

そのアイデンティティタイプで使用可能なアイデンティティのリストが、[Umbrellaポリシーに転送されるトラフィック (Traffic directed to Umbrella policy)] に表示されます。



3. Secure Access にトラフィックをリダイレクトするアイデンティティを選択します。



4. 選択したアイデンティティを [Secure Accessポリシーに転送されるトラフィック (Traffic directed to Secure Access policy)] に移動するには、矢印をクリックします。

Traffic directed to Umbrella policy

☐ Select all

Search



No identities selected

Traffic directed to Secure Access policy

☐ Select all (2 total)

Search

☐ Network 2
☐ Network 3

<
>

Redirect traffic (2)

5. [トラフィックのリダイレクト (Redirect Traffic)] をクリックします。
6. ポップアップメッセージに次のように表示されます。次のアイデンティティおよび送信元トラフィックは、**Secure Access** または **Cisco Umbrella** にリダイレクトされます。

Redirect Traffic

The following identity and source traffic will be redirected to Secure Access or Umbrella.

To Umbrella

To Secure Access

2 Networks

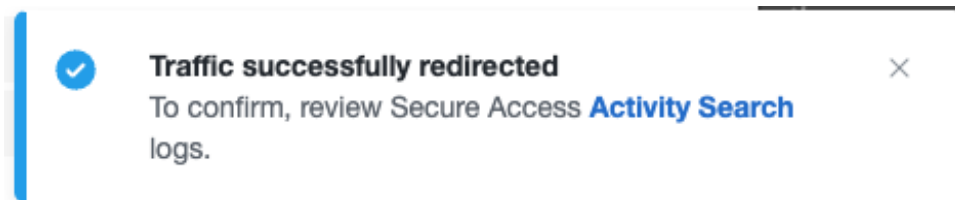
☒ I understand and wish to proceed

Cancel

Redirect

7. [理解したうえで続行します (I understand and wish to proceed)] にチェックを入れます。
8. [リダイレクト (Redirect)] をクリックします。

認証が完了すると、成功モーダルが表示されます：[トラフィックが正常にリダイレクトされました (Traffic successfully redirected)]。



Secure Access でアクティビティ検索レポートを表示し、送信元トラフィックが正常にリダイレクトされていることを確認します。左側のナビゲーションで、[Secure Access] > [レポート (Reports)] > [アクティビティ検索 (Activity Search)] をクリックします。詳細については、「[View and Customize the Activity Search Report](#)」を参照してください。

第5

章

- :
- [Cisco Secure Access - DNS Defense](#)
□□□□□

Cisco Secure Access - DNS Defense へのアップグレード移行中のレポートについて説明します。

Cisco Secure Access - DNS Defense

すべての **Cisco Umbrella** レポートを **Secure Access - DNS Defense** で利用できます。

最大で過去 **90** 日間の範囲で、特定の期間のレポートを生成できます。

詳細については、「[Monitor Secure Access with Reports](#)」を参照してください。

アップグレードマネージャの実行中は、[適用ポイント (Point of Enforcement)] フィルタを使用して、レポートで **Secure Access** と **Cisco Umbrella** の使用状況をモニターできます。[適用ポイント (Point of Enforcement)] フィルタでは、表示する製品のトラフィックパスを選択できます。

Point of Enforcement

[Select All](#)

- ☐ Cisco Umbrella
- ☐ Cisco Secure Access

重要

Cisco Umbrella を完全にシャットダウンすると、[適用ポイント (Point of Enforcement)] フィルタは使用できなくなります。詳細については、「[アップグレードを完了して Umbrella を閉じる](#)」を参照してください。

第

6

Umbrella

章

:

- [Cisco Umbrella](#) □□□□

アップグレードプロセスを完了するための最後のステップです。

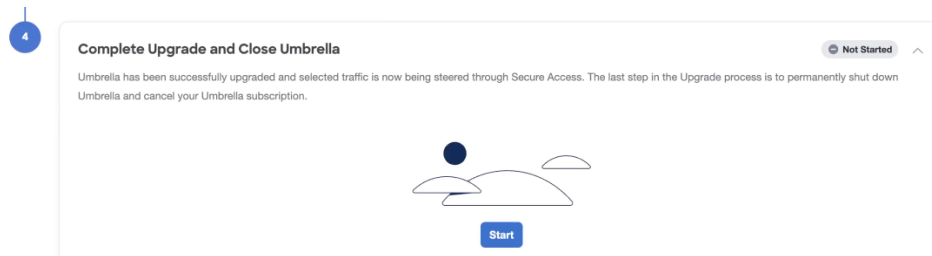
最後のステップでは、前提条件を満たし、すべてのポリシールールをアップグレードして、すべてのトラフィックを **Secure Access** に転送した後に、**Cisco Umbrella** アカウントを閉鎖します。

Cisco Umbrella

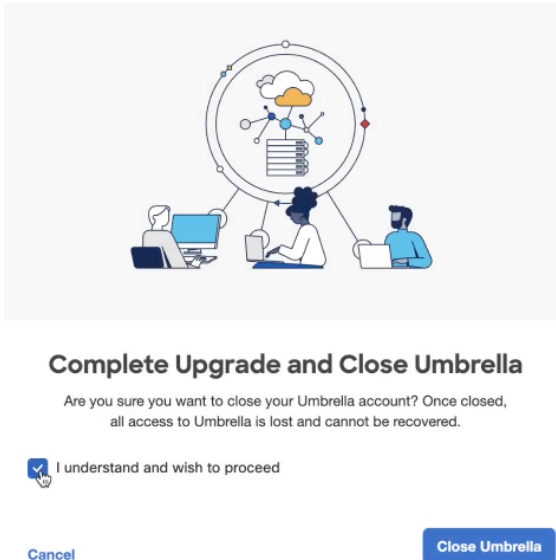
これは、Cisco Umbrella をシャットダウンし、Cisco Umbrella サブスクリプションをキャンセルする最後の手順です。

Cisco Umbrella が正常にアップグレードされ、選択したトラフィックが Secure Access を介してステアリングされるようになりました。アップグレードマネージャの最後の手順は、Cisco Umbrella を完全にシャットダウンし、Cisco Umbrella サブスクリプションをキャンセルすることです。

1. [開始 (Start)] をクリックします。



2. [理解したうえで続行します (I understand and wish to proceed)] にチェックを入れます。



3. [Umbrellaを閉じる (Close Umbrella)] をクリックします。

Cisco Umbrella アカウントが閉鎖され、組織は Secure Access - DNS Defense で完全に保護されています。

第7

章

$$\vdots$$

- [illegible]

Cisco Umbrella DNS から Cisco Secure Access - DNS Defense にアップグレードする際のトラブルシューティングのヒント。

次のトピックでは、アップグレード時にトラブルシューティングが必要になる可能性のあるシナリオについて説明します。

アップグレード中に問題が発生した場合は、このトピックのシナリオを確認してください。

問題	ソリューション
Security Cloud Control (SCC) のサブスクリプション要求コードを受信していない場合はどうすればよいですか。	• スパムの受信トレイを確認してください。 • 購入時に、そのアカウントにリンクされている管理者ではなかった可能性があります。詳細については、営業担当者にお問い合わせください。
ステップ 2 の [アップグレードを開始 (Start Upgrade)] で [アップグレードに失敗しました (Upgrade Failed)] と表示される場合はどうすればよいですか。	アップグレードプロセス中に別の管理者がポリシーを編集または追加しようとした場合、ポリシーの変換に失敗する可能性があります。アップグレードのステップ 2 を再試行する前に、Web ブラウザを更新するか、ポリシーを削除してください。
組織名を変更できますか。	• Security Cloud Control で組織名を変更するには、左側の列で組織を選択し、[プラットフォーム管理 (Platform management)] > [製品サブスクリプション (Product Subscriptions)] > [サブスクリプション (Subscriptions)] > 鉛筆アイコンをクリックして編集 > [保存 (Save)] の順に選択します。 • SCC で組織名を変更しても、Secure Access でその名前は変更されません。変更を要求するには、Secure Access サポートにお問い合わせください。
Cisco Umbrella 管理者は Cisco Umbrella ダッシュボードからロックアウトされています。	Cisco Umbrella 管理者に招待を送信して、各自の Security Cloud Control アカウントを作成してもらう必要があります。認証は今後、Security Cloud Control を介して行われます。「 Invite a User 」を参照してください。
Secure Access にアップグレードするために [招待を要求 (Request Invitation)] をクリックしたものの、サブスクリプション要求コードが記載された最初の Security Cloud Control メールを受信した管理者ではない場合はどうなりますか。	最初の Security Cloud Control メールを受信した管理者にアカウントの作成を依頼し、新規ユーザーとして追加してもらいます。その後、SCC にサブスクリプション要求コードを入力して、Secure Access へのアップグレードをアクティブ化します。
既存のインスタンスにアタッチする代わりに、新しい Secure Access インスタンスを誤って作成した場合はどうなりますか。	Secure Access サポート へのお問い合わせ
サブスクリプション要求コードを誤った Cisco Umbrella 組織にリンクした場合はどうなりますか。	Secure Access サポート へのお問い合わせ
技術的な問題がある場合は、どこに問い合わせればよいですか。	Secure Access サポート へのお問い合わせ

翻訳について

このドキュメントは、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。

翻訳について

このドキュメントは、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。